Claims

What Is Claimed Is:

1. A method for determining validity of a certificate in a system employing cross certification among certificate issuing units comprising the steps of:

for a community of interest, collecting at least one cross certificate associated with an anchor certificate issuing unit, and obtaining at least one certificate issuing unit public key and an associated unique identifier fora cross-certified certificate issuing unit identified by the at least one cross certificate; and

creating a signed certificate set identifying certificate issuing units determined to be trusted by the anchor certificate issuing unit, based on the at least one cross certificate, wherein the signed certificate set includes at least the unique identifier and the public key of each trusted certificate issuing unit.

2. The method of claim 1 including the step of generating a signed certificate set revocation list containing at least an identifier of at least one signed certificate set that has been revoked.

3. The method of claim 1 wherein the step of collecting at least one of the plurality of cross certificates includes obtaining chained cross certificates from a plurality of certificate issuing units.

4. The method of claim 1 including the step of publishing the signed certificate set of certificate issuing units wherein the published signed certificate set is accessible by a plurality of different clients units.

5. The method of claim 1 including the steps of:

generating a signed certificate set of certificate issuing units in response to requests by one or more client units;

distributing the signed certificate set to client units; and

publishing the signed certificate set generated in response to client requests, wherein the published signed certificate set is accessible by a plurality of different clients units.

6. The method of claim 1 wherein the step of collecting the plurality of cross certificates includes collecting cross certificates from a data repository associated with the anchor CA.

7. The method of claim 1 including the step of digitally signing the created signed certificate set of certificate issuing units trusted by the anchor certificate issuing unit to provide a trusted cross certificate signed certificate set for use by a client unit.

8. The method of claim 1 including the step of adding at least one of a validity period, serial number, set extension, and policy identifier to the created signed certificate set.

9. The method of claim 4 including the step of determining, by a client unit if the signed certificate set of trusted certificate issuing units is revoked and whether the signed certificate set needs to be regenerated for the anchor certificate issuing unit.

10. The method of claim 1 wherein the step of creating the signed certificate set of certificate issuing units trusted by the anchor certificate issuing unit includes generating a plurality of signed certificate sets on a per anchor certificate issuing unit basis wherein each signed certificate set contains at least: a list of unique identifiers and associated public keys of each certificate issuing units trusted by an anchor certificate issuing unit, and a digital signature of a trusted entity and a signed certificate set identifier associated with a given anchor certificate issuing unit.

11. The method of claim 1 including the step of generating a signed certificate set containing zero or more of the following: signed certificate set extensions, a signed

certificate set serial number generated each time a signed certificate set is published, an indication of the date and time at which a new signed certificate set is to be issued, an identifier that indicates where corresponding signed certificate set revocation list is posted, one or more identifiers that indicates the policy constraints under which the list of trusted CA's was constructed.

12. The method of claim 1 including the steps of:

creating a plurality of signed certificate sets on a per anchor certificate issuing unit basis wherein each signed certificate set contains at least: a list of unique identifiers and associated public keys of each certificate issuing units trusted by an anchor certificate issuing unit, and

publishing each signed certificate set wherein each published signed certificate set is accessible by a plurality of different clients units.

13. The method of claim 12 wherein the step of creating the plurality of signed certificate sets on a per anchor certificate basis includes validating a digital signature associated with each cross certificate for a given anchor certificate issuing unit and including on a signed certificate set, only those certificate issuing units that had valid certificates.

14. The method of claim 1 including the step of caching, by a client unit, a copy of the signed certificate set of certificate issuing units trusted by the anchor certificate issuing unit and wherein the client unit does not perform validation of certificate issuing unit certificates but validates an end-entity certificate by seeing if the certificate issuing entity associated with the end-entity is on the cached signed certificate set and using the public key of that certificate issuing entity to validate the end-entity certificate

15. The method of claim 1 including the step, when identifying trusted certificate issuing unit certificates, of applying policy constraints applicable for a particular trust anchor or a particular group of end entities or a particular group of client applications,

including the step of placing identifiers of those policy constraints in the signed certificate set that contains the list of trusted certificate issuing units.

16. An apparatus for use in determining validity of a certificate in a system employing trusted paths comprising:

a signed certificate set generator operative to collect at least one cross certificate associated with at least one anchor certificate issuing unit, and obtain at least one certificate issuing unit public key and an associated unique identifier for a cross-certified certificate issuing unit identified by the at least one cross certificate; and operative to create a signed certificate set identifying certificate issuing units determined to be trusted by the anchor certificate issuing unit, based on the at least one cross certificates, wherein the signed certificate set includes at least a unique identifier and public key of each trusted certificate issuing unit.

17. The apparatus of claim 16 wherein the signed certificate set generator generates and publishes a signed certificate set revocation list containing at least an identifier of at least one signed certificate set that has been revoked.

18. The apparatus of claim 16 wherein the signed certificate set generator obtains chained cross certificates from a plurality of certificate issuing units to collect the plurality of cross certificates.

19. The apparatus of claim 16 wherein the signed certificate set generator publishes the signed certificate set of certificate issuing units wherein the published signed certificate set is accessible by a plurality of different clients units.

20.The apparatus of claim 16 wherein the signed certificate set generator collects cross certificates from a data repository associated with the anchor CA.

21. The apparatus of claim 16 wherein the signed certificate set digitally signs the created signed certificate set of certificate issuing units trusted by the anchor certificate issuing unit to provide a trusted cross certificate signed certificate set for use by a client unit.

22. The apparatus of claim 16 wherein the signed certificate set generator adds at least one of a validity period, serial number, set extension, and policy identifier to the created signed certificate set.

23. The apparatus of claim 16 wherein the signed certificate set generator generates a plurality of signed certificate sets on a per anchor certificate issuing unit basis wherein each signed certificate set contains at least: a list of unique identifiers and associated public keys of each certificate issuing units trusted by an anchor certificate issuing unit, signed certificate set extensions , a signed certificate set serial number generated each time a signed certificate set is published, a digital signature of a trusted entity and a signed certificate set identifier associated with a given anchor certificate issuing unit.

24. The apparatus of claim 16 wherein the signed certificate set generator:

creates a plurality of signed certificate sets on a per anchor certificate issuing unit basis wherein each signed certificate set contains at least: a list of unique identifiers and associated public keys of each certificate issuing units trusted by an anchor certificate issuing unit, and

publishes each signed certificate set wherein each published signed certificate set is accessible by a plurality of different clients units.

25. The apparatus of claim 23 wherein the signed certificate set generator creates the plurality of signed certificate sets on a per anchor certificate basis by validating a digital signature associated with each cross certificate for a given anchor certificate issuing unit and including on a signed certificate set, only those certificate issuing units that had valid certificates.

26. A trusted public key certificate system comprising:

a signed certificate set generator operative to collect a plurality of cross certificates associated with at least one anchor certificate issuing unit, and obtain a plurality of certificate issuing unit public keys and associated unique identifiers for cross-certified certificate issuing units identified by the plurality of cross certificate; and operative to create a signed certificate set identifying certificate issuing units determined to be trusted by the anchor certificate issuing unit, based on the cross certificates, wherein the signed certificate set includes at least a unique identifier and public key of each trusted certificate issuing unit; and

at least one client unit in operative communication with the signed certificate set generator and operative to access the signed certificate set and to determine whether a received message is from a trusted source based on the signed certificate set.

27. The system of claim 26 wherein the signed certificate set generator generates a signed certificate set revocation list containing at least an identifier of at least one signed certificate set that has been revoked.

28. The system of claim 27 wherein the signed certificate set generator publishes the signed certificate set of certificate issuing units wherein the published signed certificate set is accessible by a plurality of different clients units.

29. The system of claim 26 wherein the signed certificate set generator:

creates a plurality of signed certificate sets on a per anchor certificate issuing unit basis wherein each signed certificate set contains at least: a list of unique identifiers and associated public keys of each certificate issuing units trusted by an anchor certificate issuing unit, and

publishes each signed certificate set wherein each published signed certificate set is accessible by a plurality of different clients units.

30. A storage medium comprising:

memory containing executable instructions that when read by one or more processors, causes the one or more processors to:

for a community of interest, collect at least one cross certificate associated with at least one anchor certificate issuing unit, and obtain at least one certificate issuing unit public key and associated unique identifier for a cross-certified certificate issuing unit identified by the cross certificate; and

create a signed certificate set identifying certificate issuing units determined to be trusted by the anchor certificate issuing unit, based on the at least one cross certificate, wherein the signed certificate set includes at least a unique identifier and public key of each trusted certificate issuing unit.

31. The storage medium of claim 30 wherein the memory contains executable instructions that when read by one or more processors, causes the one or more processors to:

generate a signed certificate set revocation list containing at least an identifier of at least one signed certificate set that has been revoked.

32. The storage medium of claim 30 wherein the memory contains executable instructions that when read by one or more processors, causes the one or more processors to:

publish the signed certificate set of certificate issuing units wherein the published signed certificate set is accessible by a plurality of different clients units.

33. The storage medium of claim 30 wherein the memory contains executable instructions that when read by one or more processors, causes the one or more processors to digitally sign the created signed certificate set of certificate issuing units trusted by the anchor certificate issuing unit to provide a trusted cross certificate signed certificate set for use by a client unit.

34. The storage medium of claim 30 wherein the memory contains executable instructions that when read by one or more processors, causes the one or more processors to add at least one of a validity period, serial number, set extension, and policy identifier to the created signed certificate set.

35. The storage medium of claim 30 wherein the memory contains executable instructions that when read by one or more processors, causes the one or more processors to:

create a plurality of signed certificate sets on a per anchor certificate issuing unit basis wherein each signed certificate set contains at least: a list of unique identifiers and associated public keys of each certificate issuing units trusted by an anchor certificate issuing unit, and

publish each signed certificate set wherein each published signed certificate set is accessible by a plurality of different clients units.

36. The storage medium of claim 30 wherein the memory contains executable instructions that when read by one or more processors, causes the one or more processors to collect all cross certificates associated with the at least one anchor certificate issuing unit and obtaining all certificate issuing unit certificates identified by the cross certificates.

37. The storage medium of claim 30 wherein the memory contains executable instructions that when read by one or more processors, causes the one or more processors to:

generate a signed certificate set of certificate issuing units in response to requests by one or more client units;

distribute the signed certificate set to client units; and

publish the signed certificate set generated in response to client requests, wherein the published signed certificate set is accessible by a plurality of different clients units.

5